

Growth Results and Euclidean Ideals

Hester Graves

August 17, 2010

Abstract

Lenstra's concept of Euclidean ideals generalizes the Euclidean algorithm; a domain with a Euclidean ideal has cyclic class group, while a domain with a Euclidean algorithm has trivial class group. This paper generalizes Harper's variation of Motzkin's lemma to Lenstra's concept of Euclidean ideals and then uses the large sieve to obtain growth results. It concludes that if a certain set of primes is large enough, then the ring of integers of a number field with cyclic class group has a Euclidean ideal.

1 Introduction

If a Dedekind domain R has a Euclidean algorithm, then R is principal and the class group is trivial. Lenstra generalized the concept of the Euclidean algorithm from a function defined on elements to a function defined on ideals via the concept of the Euclidean ideal. If R has a Euclidean ideal C , then $[C]$ generates the class group of R and Cl_R is cyclic. In the case where R is the ring of integers of a number field, he proved something much stronger.

Theorem 1. [7](Lenstra 1979) *Suppose K is a number field, $|\mathcal{O}_K^\times| = \infty$, and C is an ideal of \mathcal{O}_K . If one assumes the generalized Riemann hypothesis, then C is a Euclidean ideal if and only if $\text{Cl}_K = \langle [C] \rangle$.*

In this paper, we will try to prove the above theorem in certain situations without using the Riemann hypothesis. We will do this by generalizing the machinery Harper used in his dissertation to study Euclidean rings. Our first result is the following.

Theorem 2. Suppose K is a number field, $|\mathcal{O}_K^\times| = \infty$, and C is an ideal of \mathcal{O}_K . If $[C]$ generates the class group of K and

$$\{\text{primes } \mathfrak{p} \in \mathcal{O}_K \mid [\mathfrak{p}] = [C], \mathcal{O}_K^\times \rightarrow (\mathcal{O}_K/\mathfrak{p})^\times\} \gg \frac{x}{\log^2 x},$$

then C is a Euclidean ideal.

2 Euclidean Ideals

Notation: Given a Dedekind domain R , we define $E := \{\text{ideals } I : R \subset I\}$. In other words, E is the set of fractional ideals that contain R .

Given a number field K , we denote its class group by Cl_K , its class number by h_K , and its conductor by $f(K)$.

Definition 1. ([7]) Suppose R is a Dedekind domain. If C is an ideal of R , it is called Euclidean if there exists a function $\psi : E \rightarrow W$, W a well-ordered set, such that for all $I \in E$ and all $x \in IC \setminus C$, there exists some $y \in C$ such that

$$\psi((x + y)^{-1}IC) < \psi(I).$$

We say ψ is a Euclidean algorithm for C and C is a Euclidean ideal.

Proposition 1. ([7]) If R is a Dedekind domain with a Euclidean ideal C , then $[C]$ generates the class group of R .

Proposition 2. ([7]) If K is an imaginary quadratic number field and the ring of integers \mathcal{O}_K has a Euclidean ideal, then K is either $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, or $\mathbb{Q}(\sqrt{-15})$.

Definition 2. (A Motzkin-type Construction for Ideals)

Given a Dedekind domain R and some non-zero ideal C , we define

$$A_{0,C} := \{R\},$$

$$A_{i,C} := A_{i-1,C} \cup \left\{ I \mid \begin{array}{l} I \in E \text{ and } \forall x \in IC \setminus C, \exists y \in C \\ \text{such that } (x + y)^{-1}IC \in A_{i-1,C} \end{array} \right\} \text{ for } i > 0,$$

$$\text{and } A_C := \bigcup_{i=0}^{\infty} A_{i,C}.$$

Note that the $A_{i,C}$'s are nested.

Lemma 1. (A Motzkin-type Lemma for ideals)

Suppose R is a Dedekind domain and C is a non-zero ideal. If the sets A_C and E are equal, then C is a Euclidean ideal.

Proof. We shall define $\phi_C : E \longrightarrow \mathbb{N}$ by $\phi_C(I) = i$ if $I \in A_{i,C} \setminus A_{i-1,C}$. We will prove that C is Euclidean by showing that ϕ_C is a Euclidean algorithm for C . Suppose that I is an ideal in E and that x is an element in $IC \setminus C$. Since the ideal I is in A_C , there exists some y in C such that $(x + y)^{-1}IC$ is an element of $A_{\phi_C(I)-1,C}$. We conclude that there exists some y in C such that

$$\phi_C((x + y)^{-1}IC) \leq \phi_C(I) - 1 < \phi_C(I).$$

The function ϕ_C is thus a Euclidean algorithm for C and C is a Euclidean ideal. \square

2.1 Properties of IC/C

Definition 3. Suppose that C is a non-zero ideal, that I and J are ideals in E , and that α is an element of $IC \setminus C$. The ideal J is similar to α modulo IC and C , or $J \sim \alpha \pmod{IC, C}$, if J can be written as $(\alpha + y)^{-1}IC$ for some y in C .

Lemma 2. Suppose that R is a Dedekind domain, that C is a non-zero ideal, and that I is an ideal in E . If x is an element of IC , then \bar{x} generates IC/C as an R/I module if and only if $(x, C) = IC$. Furthermore, if $(x, C) = IC$ and ϕ is any R -isomorphism from $(IC/C)^{-1}$ to R/I^{-1} , then $[\phi(x)]$ is a unit in R/I^{-1} .

Proof. It is clear that the ideal C is contained in the ideal (x, C) , which is itself contained in IC . Let \bar{x} generate IC/C as an R/I^{-1} module. Therefore, for any z in $IC \setminus C$, there exists some $a \in R$ such that $\bar{z} = [a]\bar{x}$. This implies that there exists some y in C such that $z = ax + y$ and so IC is contained in (x, C) . We conclude that (x, C) is equal to IC .

Let the ideal $(x, C) = IC$, so that x is not in C , and let \bar{z} be any non-zero element of IC/C . There exists some a in R and some y in C such that $z = ax + y$, implying that $\bar{z} = [a]\bar{x}$. We conclude that \bar{x} generates IC/C as an R/I module.

Let the function $\phi : IC/C \longrightarrow R/I^{-1}$ be an isomorphism of R/I^{-1} modules. If \bar{x} generates IC/C as an R/I^{-1} module, then $\phi(\bar{x})$ generates R/I^{-1} as an R/I^{-1} module. In other words, $[\phi(x)]$ is a unit in R/I^{-1} . \square

Lemma 3. Suppose that R is a Dedekind domain, that I is an ideal in E , and that x is an element of IC such that $(x, C) = IC$. If \mathfrak{p} is a prime ideal such that $v_{\mathfrak{p}}(I^{-1}) \neq 0$, then \mathfrak{p} and $xI^{-1}C^{-1}$ are relatively prime.

Proof. If \mathfrak{p} is a prime ideal and I^{-1} is contained in \mathfrak{p} , then the ring R is contained in $\mathfrak{p}I$ and C is contained in $\mathfrak{p}IC$. Suppose that the integral ideal $xI^{-1}C^{-1}$ is also contained in \mathfrak{p} , implying that the element x would be contained in $\mathfrak{p}IC$, so the ideal (x, C) would be contained in $\mathfrak{p}IC$. This is a contradiction, so the ideals $xI^{-1}C^{-1}$ and \mathfrak{p} must be relatively prime. \square

Lemma 4. *Suppose that K is a number field and that I be an ideal in E , $I \neq R$. If x is an element of IC and $(x, C) = IC$, then the set of prime ideals \mathfrak{p} such that $\mathfrak{p}^{-1} \sim x \pmod{IC, C}$ is of positive density in the set of all prime ideals. In other words, there is a positive density of prime ideals \mathfrak{p} such that $\mathfrak{p}^{-1} = (x + y)^{-1}IC$ for some y in C .*

Proof. (Proof of Lemma 4) Suppose that $K^{I^{-1}}$ is the ray class field of K of modulus I^{-1} and that x is an element of IC such that $(x, C) = IC$. We know by Lemma 3 that (x, C) is relatively prime to any prime ideal \mathfrak{p} such that \mathfrak{p} divides I^{-1} , so the integral ideal $xI^{-1}C^{-1}$ is in the domain of the Artin map (i.e. $\mathbb{I}^{S(I^{-1})}$) for $K^{I^{-1}}$. We shall call the support of the modulus $S(I^{-1})$ and we shall call this Artin map $\psi_{K^{I^{-1}}}$.

The Chebotarev density theorem implies that there is a positive density of prime ideals \mathfrak{q} in the preimage of $\psi_{K^{I^{-1}}}(xI^{-1}C^{-1})$ in the set of all prime ideals. Each of these ideals \mathfrak{q} can be written as $(1 + q)xI^{-1}C^{-1}$ for some q , where $v_{\mathfrak{p}}(q) \geq v_{\mathfrak{p}}(I^{-1})$ for all primes \mathfrak{p} in $S(I^{-1})$. Note that $(x + xq) = (1 + q)x = \mathfrak{q}IC$, so that $x + xq$ is an element of IC . We chose x to be an element of IC , so xq is also an element of IC . As such, we know that $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(IC)$ for all primes \mathfrak{p} . Note this implies that $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(C)$ for $\mathfrak{p} \notin S(I^{-1})$ because $v_{\mathfrak{p}}(I) = 0$. Since x is an element of IC , we know that $v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(IC)$ for all primes \mathfrak{p} . We know that $v_{\mathfrak{p}}(q) \geq v_{\mathfrak{p}}(I^{-1})$ for all primes \mathfrak{p} in $S(I^{-1})$, so that $v_{\mathfrak{p}}(xq) = v_{\mathfrak{p}}(q) + v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(I^{-1}) + v_{\mathfrak{p}}(IC) = v_{\mathfrak{p}}(C)$ for primes \mathfrak{p} in $S(I^{-1})$. We conclude that, because $v_{\mathfrak{p}}(xq) \geq v_{\mathfrak{p}}(C)$ for all primes \mathfrak{p} , xq is an element of C , so that $\mathfrak{q} = (x + xq)I^{-1}C^{-1}$, where xq is an element of C . We conclude that $\mathfrak{q}^{-1} \sim x \pmod{IC, C}$. \square

Definition 4. *For any $I \in E$ that is equivalent to C^n , $h_K \geq n > 0$, fix some $x_I \in K^\times$ such that $I = x_{I^{-1}}^{-1}C^n$.*

Henceforth, assume that C is an integral ideal. This means that $(x_{I^{-1}}) = I^{-1}C^n$, so that $x_{I^{-1}}$ is an element of C^n and is therefore an integer.

Lemma 5. *Given two elements x and y in C^n , $n \geq 0$, $x \equiv y \pmod{\mathfrak{p}C^n}$ if and only if $x \equiv y \pmod{\mathfrak{p}}$.*

Proof. Since $x \equiv y \pmod{\mathfrak{p}C^n}$, then $x - y$ is in $\mathfrak{p}C^n$ and is therefore in \mathfrak{p} , so $x \equiv y \pmod{\mathfrak{p}}$.

Conversely, suppose $x \equiv y \pmod{\mathfrak{p}}$. Then $x - y \in \mathfrak{p}$, but we also know that $x - y \in C^n$ because both $x, y \in C^n$. As $x - y$ is in both \mathfrak{p} and C^n , it is in the intersection of \mathfrak{p} and C^n . We know that \mathfrak{p} and C are relatively prime, so \mathfrak{p} and C^n are relatively prime, which means that their intersection is in fact their product. We conclude that $x \equiv y \pmod{\mathfrak{p}C^n}$. \square

Lemma 6. *Suppose that \mathfrak{p} is a prime ideal such that $[\mathfrak{p}^{-1}] = [C^{n-1}]$. Given an element y in K^\times , the product $yx_{\mathfrak{p}}$ is in $\mathfrak{p}C^n$ if and only if y is an element of C .*

Proof. If y is in C , then $yx_{\mathfrak{p}}$ is an element of $(\mathfrak{p}C)(C^{n-1}) = \mathfrak{p}C^n$.

If $yx_{\mathfrak{p}}$ is an element of $\mathfrak{p}C^n$, then $(yx_{\mathfrak{p}}) = I\mathfrak{p}C^n$, for some non-zero integral ideal I . Therefore $(y) = Ix_{\mathfrak{p}}^{-1}C^{n-1}\mathfrak{p}C = I\mathfrak{p}^{-1}\mathfrak{p}C$ so that $(y) = IC$. We conclude $y \in IC$, which implies that $y \in C$. \square

Lemma 7. *Multiplication by $x_{\mathfrak{p}}$ is an isomorphism from $\mathfrak{p}^{-1}C/C$ to $C^n/\mathfrak{p}C^n$.*

Proof. Given some β in $\mathfrak{p}^{-1}C$, we know that $x_{\mathfrak{p}}\beta$ is in $\mathfrak{p}C^{n-1}\mathfrak{p}^{-1}C$, which is equal to C^n , so that multiplication by $x_{\mathfrak{p}}$ is a map from $\mathfrak{p}^{-1}C$ to C^n . Let b be an element of C^n . Then $x_{\mathfrak{p}}^{-1}b$ is an element of $\mathfrak{p}^{-1}C^{1-n}C^n = \mathfrak{p}^{-1}C$, so that multiplication by $x_{\mathfrak{p}}$ is surjective.

By Lemma 6, the product $yx_{\mathfrak{p}}$ is in $\mathfrak{p}C^n$ if and only if y is in C , so that $x_{\mathfrak{p}}^{-1}\mathfrak{p}C^n$ is C , and the kernel of the composition of multiplication by $x_{\mathfrak{p}}$ and taking the quotient of $\mathfrak{p}^{-1}C$ by C is $\mathfrak{p}C^n$. The isomorphism follows. \square

3 Growth Results

Definition 5. *Given a Dedekind domain R and a non-zero ideal C , we define*

$$B_{0,C} := \{R\},$$

$$B_{i,C} = B_{i-1,C} \cup \left\{ \mathfrak{p}^{-1} \left| \begin{array}{l} \mathfrak{p} \subseteq R \text{ is prime, and} \\ \forall x \in \mathfrak{p}^{-1}C \setminus C, \exists y \in C \text{ such} \\ \text{that } (x - y)^{-1}\mathfrak{p}^{-1}C \in B_{i-1,C} \end{array} \right. \right\} \text{ for } i > 0,$$

$$\text{and } B_C := \bigcup_{i=0}^{\infty} B_{i,C}.$$

Theorem 3. *Suppose that K is a number field and that C is a non-zero ideal of \mathcal{O}_K . If B_C contains all ideals \mathfrak{p}^{-1} such that \mathfrak{p} is prime, then C is a Euclidean ideal.*

Proof. The techniques of this proof follow those in [4], however we use Lemma 4 instead of Dirichlet's theorem on primes in arithmetic progressions.

Define ω to be the function mapping from E to \mathbb{N} such that $\omega(I)$ is the number of prime divisors of I^{-1} , with multiplicity. If \mathfrak{p} is a prime ideal, define $\lambda(\mathfrak{p}^{-1}) := i$ if \mathfrak{p}^{-1} is an element of $B_{i,C} \setminus B_{i-1,C}$. Extend λ to all of E by additivity. We then combine the two functions together as $\phi : E \rightarrow \mathbb{N} \times \mathbb{N}$, with $\phi(I) = (\omega(I), \lambda(I))$, and order the image $\phi(E)$ lexicographically. Because both ω and λ are additive functions, the function ϕ is additive as well. Note that $\phi(I) = (0, 0)$ if and only if $I = \mathcal{O}_K$.

In order to prove Theorem 3, it suffices to show that ϕ is a Euclidean algorithm with respect to C , which we shall prove by induction. Suppose that \mathfrak{p} is a prime ideal and that $\phi(\mathfrak{p}^{-1}) = (1, i)$. For any x in $\mathfrak{p}^{-1}C \setminus C$, there exists some y such that $(x + y)^{-1}\mathfrak{p}^{-1}C$ is an element of $B_{i-1,C}$, so that $\phi((x + y)^{-1}\mathfrak{p}^{-1}C) = (0, 0)$ or $\phi((x + y)^{-1}\mathfrak{p}^{-1}C) = (1, j)$, where $j < i$.

Let I be an element of E with I^{-1} not a prime ideal. Suppose that for all J such that $\phi(J) < \phi(I)$ and for all a in $JC \setminus C$, there exists some y in C such that $\phi((x + y)^{-1}JC) < \phi(J)$. If $x \in IC \setminus C$ and $(x, C) = IC$, we can apply Theorem 4. There exists some $y \in C$ such that $(x + y)^{-1}IC = \mathfrak{p}^{-1}$, where \mathfrak{p} is a prime ideal. Since $\phi(\mathfrak{p})$ is less than $\phi(I)$, the condition is satisfied.

If $x \in IC \setminus C$ and (x, C) is not equal to IC , then we define L to be $(I^{-1}, xI^{-1}C)$. The integral ideal L contains I^{-1} , so $I^{-1}L^{-1}$ has fewer prime divisors (counting multiplicities) than I^{-1} and $\phi(IL)$ is less than $\phi(I)$. There exists some y in C such that $\phi((x + y)^{-1}ILC) < \phi(IL)$. The additivity of ϕ implies that given two ideals M and N , $\phi(MN) = \phi(M) + \phi(N)$, so $\phi((x + y)IC) < \phi(I)$ and the condition holds. We conclude that ϕ is a Euclidean algorithm for $[C]$ and that $[C]$ is a Euclidean ideal class. \square

Definition 6. Given the set $B_{i,C}$, we define

$$\begin{aligned} B_{i,C}(x) &:= \{I \in B_{i,C} \mid \text{Nm}(I^{-1}) \leq x\}, \\ B_{i,C}^c &:= \{I \in E \setminus B_{i,C} \mid [I] = [J] \text{ for any } J \in B_{i,C}\}, \text{ and} \\ B_{i,C}^c(x) &:= \{I \in B_{i,C}^c \mid \text{Nm}(I^{-1}) \leq x\}. \end{aligned}$$

Theorem 4. If K is a number field such that $|\mathcal{O}_K^\times| = \infty$, $[C]$ generates Cl_K , and if

$$|B_{1,C}(x)| \gg \frac{x}{\log^2 x},$$

then $E = A_C$ and C is a Euclidean ideal.

Corollary 1. *If K is a number field such that $|\mathcal{O}_K^\times| = \infty$, if $[C]$ generates Cl_K , and if*

$$\left| \left\{ \begin{array}{l} \text{prime ideals} \\ \mathfrak{p} \in \mathcal{O}_K \end{array} \mid \text{Nm}(\mathfrak{p}) \leq x, [\mathfrak{p}] = [C], \mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p})^\times \right\} \right| \gg \frac{x}{\log^2 x},$$

then C is a Euclidean ideal.

Proof. We will prove the corollary by proving that the ideal \mathfrak{p}^{-1} is in $B_{1,C}$ if and only if $[\mathfrak{p}] = [C]$ and $\mathcal{O}_K^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p})^\times$. Clearly \mathfrak{p}^{-1} can only belong to $B_{1,C}$ if $[\mathfrak{p}] = [C]$. For the rest of the proof, assume that $[\mathfrak{p}] = [C]$. If $C^{h_K} = (c)$, then by Lemma 7, multiplication by $\frac{x_{\mathfrak{p}}}{c}$ is an isomorphism from $\mathfrak{p}^{-1}C/C$ to $\mathcal{O}_K/\mathfrak{p}$. By definition, we know that $\mathfrak{p}^{-1} \in B_{1,C}$ if and only if for all $\beta \in \mathfrak{p}^{-1}C \setminus C$, there exists some $y \in C$ such that $(\beta + y)^{-1}\mathfrak{p}^{-1}C = \mathcal{O}_K$. We can rewrite $(\beta + y)^{-1}\mathfrak{p}^{-1}C = \mathcal{O}_K$ as $\frac{x_{\mathfrak{p}/c}}{\frac{x_{\mathfrak{p}}}{c}\beta + \frac{x_{\mathfrak{p}}}{c}y}\mathfrak{p}^{-1}C = \mathcal{O}_K$, which is equivalent to the condition $\frac{x_{\mathfrak{p}}}{c}\beta + \frac{x_{\mathfrak{p}}}{c}y \in \mathcal{O}_K^\times$, where $\frac{x_{\mathfrak{p}}}{c}\beta \in \mathcal{O}_K$ and $\frac{x_{\mathfrak{p}}}{c}y \in \mathfrak{p}$. We conclude that $(\beta + y)^{-1}\mathfrak{p}^{-1}C = \mathcal{O}_K$ if and only if the image of β under multiplication by $\frac{x_{\mathfrak{p}}}{c}$ is congruent to a unit of \mathcal{O}_K modulo \mathfrak{p} . \square

In order to prove Theorem 4, we will first need to state the Gupta-Murty bound and the Large Sieve for ideals.

4 The Gupta-Murty Bound

In order to state the Gupta-Murty bound, we need the following definitions.

Given a prime ideal \mathfrak{p} , define $q_{\mathfrak{p}} : \mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$ to be the quotient map where \mathfrak{p} is the kernel. Using our new notation for the quotient map, we can now define an important constant for \mathcal{O}_K and \mathfrak{p} .

Definition 7. *Given a prime ideal \mathfrak{p} , we define $f(\mathfrak{p}) := |q_{\mathfrak{p}}(\mathcal{O}_K^\times)|$.*

The constant $f(\mathfrak{p})$ is the size of the image of the units under the quotient group, which is bounded above by the size of the set of the units in $\mathcal{O}_K/\mathfrak{p}$. The constant $f(\mathfrak{p})$ is a special case of the following.

Definition 8. *Suppose that K is a number field and \mathfrak{p} a prime ideal of \mathcal{O}_K . If \mathfrak{M} is a monoid in \mathcal{O}_K such that $\mathfrak{M} \cap \mathfrak{p} = \emptyset$, then we define $f_{\mathfrak{M}}(\mathfrak{p})$ to be $|q_{\mathfrak{p}}(\mathfrak{M})|$.*

The quantity $f(\mathfrak{p})$ is therefore the same as $f_{\mathcal{O}_K^\times}(\mathfrak{p})$.

Definition 9. A set of elements x_1, \dots, x_n of K is **multiplicatively independent** if the only integer n -tuple (a_1, \dots, a_n) satisfying $x_1^{a_1} \cdots x_n^{a_n} = 1$ is $(0, \dots, 0)$.

Theorem 5. (The Gupta-Murty Bound) ([3]) If \mathfrak{M} is a finitely-generated monoid in \mathcal{O}_K containing t multiplicatively independent elements, then

$$|\{\mathfrak{p} | f_{\mathfrak{M}}(\mathfrak{p}) \leq y\}| \ll y^{\frac{t+1}{t}},$$

where the implied constant depends on K , t , and the generators of \mathfrak{M} .

5 The Large Sieve for Euclidean Ideal Classes

The large sieve is at the heart of Harper's work on Euclidean rings. In order to generalize his work and examine the asymptotic growth of the sets $B_{i,C}$, a generalized large sieve is needed. Before the generalized version can be stated, however, we need the following definitions.

Definition 10. For each coset in the image of \mathcal{O}_K^\times in $(\mathcal{O}_K/\mathfrak{p})^\times$, choose one unit that maps to that coset. Let $U(\mathfrak{p})$ be the collection of those units. Note that $|U(\mathfrak{p})|$ is $f(\mathfrak{p})$.

Definition 11. Given \mathfrak{A} , a finite set of non-associated integers, a prime ideal \mathfrak{p} and some $\alpha \in \mathcal{O}_K$, we define the following function

$$Z(\alpha, \mathfrak{p}) := |\{x \in \mathfrak{A} : x \equiv \alpha \pmod{\mathfrak{p}}\}|.$$

For our purposes, we want to apply the large sieve to sets of ideals, so that we look at how a finite set of ideals are distributed among the similarity classes of finite set of prime ideals, rather than how finite sets of elements are distributed among the equivalence classes of prime ideals. We will therefore look at the function $Z(\alpha, \mathfrak{p}, C)$ rather than $Z(\alpha, \mathfrak{p})$.

Definition 12. Suppose that C is a non-zero integral ideal and that $n \in \mathbb{Z}^+$. Let A be a finite set of distinct fractional ideals I in E , such that if I and J are in A , then $[I] = [J]$. If \mathfrak{p} is a prime ideal such that $[\mathfrak{p}^{-1}] = [IC^{-1}]$ for I in A , and if β is in $\mathfrak{p}^{-1}C$, we define

$$Z(\beta, \mathfrak{p}, C) := \begin{cases} |\{I \in A | \exists y \in C \text{ such that } (\beta + y)^{-1} \mathfrak{p}^{-1} C = I\}| \\ \text{if } \beta \notin C \\ f(\mathfrak{p}) |\{I \in A | \exists y \in C \text{ such that } (\beta + y)^{-1} \mathfrak{p}^{-1} C = I\}| \\ \text{if } \beta \in C \end{cases}$$

Definition 13. Given a finite set A , such that $A \subset \{I | I \in E \text{ and } [I] = [C^n]\}$, define $\mathfrak{A} := \{x_I | I \in A\}$.

Using our notation above, we can prove the following theorem.

Theorem 6. For C a non-zero integral ideal, \mathfrak{p} a prime ideal that is relatively prime to C , and $\beta \in \mathfrak{p}^{-1}C$, we have

$$Z(\beta, \mathfrak{p}, C) = \begin{cases} \sum_{u \in U(\mathfrak{p})} Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) & \text{if } \beta \notin C \\ f(\mathfrak{p})Z(0, \mathfrak{p}) & \text{if } \beta \in C \end{cases}$$

Proof. (Proof of Theorem 6) Using the elements defined above, we can rewrite the equation

$$I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$$

as

$$x_I^{-1}C^n = (\beta + y)^{-1}x_{\mathfrak{p}}^{-1}C^{n-1}C.$$

The above statement on ideals implies that

$$ux_I = \beta x_{\mathfrak{p}} + yx_{\mathfrak{p}} \text{ for some } u \in \mathcal{O}_K^\times,$$

a statement on elements. Note that both ux_I and $\beta x_{\mathfrak{p}}$ are in C^n and that $yx_{\mathfrak{p}}$ is in $\mathfrak{p}C^n$ if and only if y is in C by Lemma 6. Therefore, the statement that there exists some

$$y \in C \text{ such that } I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$$

is equivalent to saying

$$ux_I \equiv \beta x_{\mathfrak{p}} \pmod{\mathfrak{p}C^n} \text{ for some } u \in \mathcal{O}_K^\times.$$

We know from Lemma 6 that this last condition is equivalent to

$$x_I \equiv u'\beta x_{\mathfrak{p}} \pmod{\mathfrak{p}} \text{ for some } u' \in \mathcal{O}_K^\times.$$

Note that β is in C if and only if $\beta x_{\mathfrak{p}} \equiv 0 \pmod{\mathfrak{p}C^n}$, which implies that $ux_I \equiv 0 \pmod{\mathfrak{p}C^n}$, which is true if and only if $x_I \equiv 0 \pmod{\mathfrak{p}}$ by Lemma 5. Since there exists an element y in C such that $I = (\alpha + y)^{-1}\mathfrak{p}^{-1}C$ if and only if $x_I \equiv 0 \pmod{\mathfrak{p}}$, we conclude that if β is in C , then

$$Z(\beta, \mathfrak{p}, C) = f(\mathfrak{p})|\{I \in A : \exists y \in C \text{ such that } (\beta + y)^{-1}\mathfrak{p}^{-1}C = I\}|$$

$$= f(\mathfrak{p})|\{x_I \in \mathfrak{A} : x_I \equiv 0 \pmod{\mathfrak{p}}\}| = f(\mathfrak{p})Z(\beta x_{\mathfrak{p}}, \mathfrak{p}).$$

If β is not in C , this means there exists some y in C such that $I = (\beta + y)^{-1}\mathfrak{p}^{-1}C$ if and only if $x_I \equiv u\beta x_{\mathfrak{p}} \pmod{\mathfrak{p}}$ for some $u \in \mathcal{O}_K^\times$. We conclude that if β is not in C , then

$$\begin{aligned} Z(\beta, \mathfrak{p}, C) &= |\{I \in A : \exists y \in C \text{ such that } (\alpha + y)^{-1}\mathfrak{p}^{-1}C = I\}| \\ &= |\{x_I \in \mathfrak{A} : x_I \equiv u\beta x_{\mathfrak{p}} \text{ for some } u \in \mathcal{O}_K^\times\}| \\ &= \sum_{u \in U(\mathfrak{p})} |\{x_I \in \mathfrak{A} : x_I \equiv u\beta x_{\mathfrak{p}} \pmod{\mathfrak{p}}\}| = \sum_{u \in U(\mathfrak{p})} Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}). \end{aligned}$$

□

Theorem 7. *If C is a non-zero integral ideal; if A is a finite collection of ideals, $A \subset E \cap [C^n]$; if \mathfrak{p} is a prime ideal; and if \mathfrak{p} and C are relatively prime, then*

$$\sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \leq \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

Proof. From the above, if β is in C , then

$$\left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 = \left(\frac{f(\mathfrak{p})Z(0, \mathfrak{p})}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2,$$

which equals

$$\left(Z(0, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

If β is not in C , then

$$\left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 = \left(\frac{\sum_{u \in U(\mathfrak{p})} Z(u\beta x_{\mathfrak{p}})}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

We can rewrite the right hand side as

$$\left(\sum_{u \in U(\mathfrak{p})} \left(\frac{Z(u\beta x_{\mathfrak{p}})}{f(\mathfrak{p})} - \frac{|A|}{f(\mathfrak{p})\text{Nm}(\mathfrak{p})} \right) \right)^2,$$

which equals

$$\frac{1}{(f(\mathfrak{p}))^2} \left(\sum_{u \in U(\mathfrak{p})} \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right) \right)^2.$$

If we apply Cauchy-Schwartz, we see that the above is less than or equal to

$$\frac{1}{(f(\mathfrak{p}))^2} \sum_{u \in U(\mathfrak{p})} f(\mathfrak{p}) \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 = \frac{1}{f(\mathfrak{p})} \sum_{u \in U(\mathfrak{p})} \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

Summing up over all non-zero classes β in $\mathfrak{p}^{-1}C/C$ yields

$$\begin{aligned} \sum_{\substack{\beta(\bmod C) \\ \beta \not\equiv 0(\bmod C)}} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 &\leq \frac{1}{f(\mathfrak{p})} \sum_{\substack{\beta(\bmod C) \\ \beta \not\equiv 0}} \sum_{u \in U(\mathfrak{p})} \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \\ &= \frac{1}{f(\mathfrak{p})} \sum_{u \in U(\mathfrak{p})} \sum_{\substack{\beta(\bmod C) \\ \beta \not\equiv 0}} \left(Z(u\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2. \end{aligned}$$

The inner sum is independent of choice of u so that the above is equal to

$$\frac{1}{f(\mathfrak{p})} f(\mathfrak{p}) \sum_{\substack{\beta(\bmod C) \\ \beta \not\equiv 0}} \left(Z(\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2,$$

which can be further simplified to

$$\sum_{\substack{\beta(\bmod C) \\ \beta \not\equiv 0}} \left(Z(\beta x_{\mathfrak{p}}, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 = \sum_{\substack{\alpha(\bmod \mathfrak{p}), \\ \alpha \not\equiv 0}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2$$

by Lemma 7. Finally, by considering both cases at once, we get

$$\sum_{\beta \in \mathfrak{p}^{-1}C \pmod C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \leq \sum_{\alpha(\bmod \mathfrak{p})} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

□

Theorem 8. (*Large Sieve with Respect to C*)

Suppose that A and P are finite sets of fractional ideals, with $A \subset E \cap [C^n]$ and $P \subset \{\mathfrak{p} : \mathfrak{p} \text{ is prime, } [\mathfrak{p}^{-1}] = [C^{n-1}]\}$. If $X = \max_{I \in A} \text{Nm}(I^{-1})$ and $Q = \max_{\mathfrak{p}^{-1} \in P} \text{Nm}(\mathfrak{p})$, then

$$\sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + X)|A|.$$

The implied constant depends only on K , the ideal C , and on n .

Proof. We know from Theorem 7 that

$$\sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \leq \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2.$$

This means that

$$\begin{aligned} \sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \\ \leq \sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2. \end{aligned}$$

The maximum norm of any element in \mathfrak{A} is

$$\max_{x \in \mathfrak{A}} \text{Nm}(x) = \max_{I \in A} \text{Nm}(x_I) = \text{Nm}(C^n)X.$$

Applying the large sieve, we know that

$$\sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + \text{Nm}(C)^n X)|\mathfrak{A}|.$$

The sizes of A and \mathfrak{A} are the same, so that

$$\sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\alpha \pmod{\mathfrak{p}}} \left(Z(\alpha, \mathfrak{p}) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + \text{Nm}(C)^n X)|A|,$$

where the implied constant only depends on the number field K . When we put this together with the earlier inequality, we see that

$$\sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(\frac{Z(\beta, \mathfrak{p}, C)}{f(\mathfrak{p})} - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 << (Q^2 + X)|A|,$$

with the implied constant now depending on both the choice of number field K , C , and n .

□

Harper did not use the large sieve in his paper, so much as a corollary of the large sieve. In order to state our version of the corollary, we need the following definition.

Definition 14. Let $\omega(\mathfrak{p}) := |\{[\alpha] \in \mathfrak{p}^{-1}C/C \mid Z(\alpha, \mathfrak{p}, C) = 0\}|$.

Corollary 2. Let A and P be finite sets of fractional ideals, with $A \subset E \cap [C^n]$ and $P \subset \{\mathfrak{p} \mid \mathfrak{p} \text{ is prime}, [\mathfrak{p}^{-1}] = [C^{n-1}]\}$. If $X = \max_{I \in A} \text{Nm}(I^{-1})$ and $Q = \max_{\mathfrak{p}^{-1} \in P} \text{Nm}(\mathfrak{p})$, then

$$\sum_{\mathfrak{p} \in P} \frac{\omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} \ll \frac{Q^2 + X}{|A|},$$

where the implied constant depends only on K , C , and n .

Proof. We know from Theorem 8 that

$$\begin{aligned} & \sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(Z(\beta, \mathfrak{p}, C) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 \\ & \geq \sum_{\left\{ \begin{array}{l} \beta \in \mathfrak{p}^{-1}C/C \\ Z(\alpha, \mathfrak{p}, C) = 0 \end{array} \right\}} \left(Z(\alpha, \mathfrak{p}, C) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2 = \frac{|A|^2 \omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})^2}. \end{aligned}$$

Since the quantity $\frac{|A|^2 \omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})^2}$ is less or equal to than

$$\sum_{\beta \in \mathfrak{p}^{-1}C/C} \left(Z(\alpha, \mathfrak{p}, C) - \frac{|A|}{\text{Nm}(\mathfrak{p})} \right)^2,$$

we know that

$$\sum_{\mathfrak{p} \in P} \text{Nm}(\mathfrak{p}) \frac{|A|^2 \omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})^2} \ll (Q^2 + X)|A|$$

and therefore

$$\sum_{\mathfrak{p} \in P} \frac{|A|^2 \omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} \ll (Q^2 + X)|A|.$$

We conclude that

$$\sum_{\mathfrak{p} \in P} \frac{\omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} << \frac{Q^2 + X}{|A|}.$$

□

6 Proof of Theorem 4

Proof. (Proof of Theorem 4) First we shall prove that if

$|B_{1,C}(x)| \gg \frac{x}{\log^2 x}$, then $|B_{2,C}(x)| \sim \frac{x}{h_K \log x}$. We shall define A to be the set $B_{1,C}(x^2)$, define $X \leq x^2$, and P to be the set $B_{2,C}^c(x)$, so that $Q \leq x$. By Corollary 2, we know that

$$\sum_{\mathfrak{p} \in P} \frac{\omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} << \frac{Q^2 + X}{|A|} << \frac{2x^2}{\frac{x^2}{\log^2(x^2)}} = \frac{2x^2}{\frac{x^2}{2\log^2(x)}} << \log^2(x).$$

Note that if I is in $B_{1,C}^c$, then there is some x in $IC \setminus C$ such that there is no y in C such that $(x+y)^{-1}IC = \mathcal{O}_K^\times$. Given any $u \in \mathcal{O}_K^\times$, we know that $(ux+uy)^{-1}IC = (x+y)^{-1}IC$ and that uy is in C . Therefore, if $Z(x, \mathfrak{p}^{-1}, C)$ is zero, then so is $Z(ux, \mathfrak{p}^{-1}, C)$ for any unit u . This means that if there is one x in $\mathfrak{p}^{-1}C \setminus C$ such that $Z(x, \mathfrak{p}) = 0$, then there are at least $f(\mathfrak{p})$ cosets with elements e such that $Z(e, \mathfrak{p}) = 0$, and the function $\omega(\mathfrak{p})$ is divisible by $f(\mathfrak{p})$.

If \mathcal{O}_K has infinitely many units, then

$$|\{\mathfrak{p} | \text{Nm}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| << x^{1-2\epsilon}$$

by Theorem 5 and therefore

$$|\{\mathfrak{p} | \text{Nm}(\mathfrak{p}) \leq x \text{ and } f(\mathfrak{p}) \leq \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| = o\left(\frac{x}{\log x}\right).$$

The above estimate implies that

$$\begin{aligned} \sum_{\substack{\mathfrak{p}^{-1} \in P(x) \\ f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}}} \frac{\omega(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} &\geq \sum_{\substack{\mathfrak{p}^{-1} \in P^c(x) \\ f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}}} \frac{f(\mathfrak{p})}{\text{Nm}(\mathfrak{p})} \\ &> \frac{|\{\mathfrak{p} \in B_{2,C}^c : f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|}{x^{\frac{1}{2}+\epsilon}}. \end{aligned}$$

By combining this with the first bound in the proof, we know that

$$\log^2(x) \gg \frac{|\{\mathfrak{p} \in B_{2,C}^c : f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|}{x^{\frac{1}{2}+\epsilon}}.$$

Multiplying both sides by $x^{\frac{1}{2}+\epsilon}$ yields

$$|\{\mathfrak{p} \in B_{2,C}^c : f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| = o\left(\frac{x}{\log(x)}\right).$$

Since the size of $B_{2,C}^c(x)$ is equal to

$$|\{\mathfrak{p} \in B_{2,C}^c(x) | f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| + |\{\mathfrak{p} \in B_{2,C}^c(x) | f(\mathfrak{p}) \leq \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|,$$

we know the size of $B_{2,C}^c(x)$ is less than or equal to

$$|\{\mathfrak{p} \in B_{2,C}^c(x) | f(\mathfrak{p}) > \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| + |\{\mathfrak{p} | \text{Nm}(\mathfrak{p}) \leq x, f(\mathfrak{p}) \leq \text{Nm}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|$$

and can thus conclude $|B_{2,C}^c(x)| = o\left(\frac{x}{\log(x)}\right)$ and

$$|B_{2,C}(x)| \sim \frac{x}{h_K \log x}.$$

Suppose that \mathfrak{p} is prime, that $[\mathfrak{p}] = [C^{n+2}]$, and that x is an element of $\mathfrak{p}^{-1}C \setminus C$. There is a positive density of prime ideals \mathfrak{q} such that $\mathfrak{q}^{-1} = (x+y)^{-1}\mathfrak{p}^{-1}C$ for some y in C by Theorem 4. The density of primes in $[C^{n+1}]$ in the set of all primes is $\frac{1}{h_K}$, which is the same as the density of primes \mathfrak{q} such that \mathfrak{q}^{-1} is in $B_{2,C}$, so there exists some prime \mathfrak{q} in $B_{2,C}$ such that $\mathfrak{q}^{-1} = (x+y)^{-1}\mathfrak{p}^{-1}C$ for some y in C . We conclude that \mathfrak{p}^{-1} is in $B_{3,C}$. \square

Acknowledgments This paper grew out of the author's dissertation, which would not be completed were it not for the author's advisor, Nick Ramsey, who supported and encouraged her. The author would like to thank E. Hunter Brooks, Chris Hall, Malcolm Harper, Jeffery Lagarias, and Chris Skinner for their help.

References

- [1] David A. Clark and M.Ram Murty, "The Euclidean algorithm for Galois extensions of \mathbb{Q} ," *Journal fr die reine und angewandte Mathematik* 459, 151-162, 1995.

- [2] Hester Graves and Nick Ramsey, “Euclidean Ideals in Quadratic Imaginary Fields,” in preparation.
- [3] Rajiv Gupta and M. Ram Murty, “A Remark on Artin’s Conjecture,” *Invent. Math* 78, 127-130, 1984.
- [4] M. Harper, “ $\mathbb{Z}[\sqrt{14}]$ is Euclidean,” *Canad. J. Math* 56, 55-70, 2004.
- [5] M. Harper and M. Ram Murty, “Euclidean rings of algebraic integers,” *Canad. J. Math* 56, 71-76, 2004.
- [6] K. Ireland and M. Rosen, “A Classical Introduction to Modern Number Theory,” Springer-Verlag, New York, NY, 1990.
- [7] H.K. Lenstra, “Euclidean Ideal Classes,” *Asterique* 61, 121-131, 1979.
- [8] Th. Motzkin, ”The Euclidean Algorithm,” *Bull. Amer. Math. Soc.* 55, 1142-6, 1949.
- [9] P. Samuel, “About Euclidean Rings,” *Journal of Algebra* 19, 282-301, 1971.
- [10] Peter J. Weinberger, “On Euclidean rings of algebraic integers”, *Proceedings of Symposia in Pure Mathematics (AMS)* 24: 321-332, 1973.
- [11] Robin J. Wilson, “The large sieve in algebraic number Fields”, *Mathematika* 16, 189-204, 1969.